

An Autonomous Attestation Token to Secure Mobile Agents in Disaster Response

Daniel Hein, Ronald Toegl

daniel.hein@iaik.tugraz.at

Institute for Applied Information Processing and
Communications (IAIK)

Graz University of Technology

Outline I

Mobile Agents

- Security issues

Trusted Computing

- Platform measurement
- Platform reporting

Mobile Agents in disaster response

- Scenario

Outline II

Local Attestation

- Autonomous Attestation Token

Attestation based key release protocol

Autonomous Attestation Token hardware

- Requirements
- Architecture

Conclusion

Mobile Agents

Mobile Agent

- *Self-contained and identifiable computer programs that move within a network and act on behalf of a user or another entity [RS98]*

Mobile Agents combine

- Code mobility
- User task delegation

Agents should be

- Autonomous
- Interactive
- Adaptable

Mobile Agents

Mobile Agents

- Travel between machines and
- Act on behalf of a user

Advantages

- Network traffic reduction
- Asynchronous interaction

Agent Execution Environment

- Executes Mobile Agents

Mobile Agent Platform

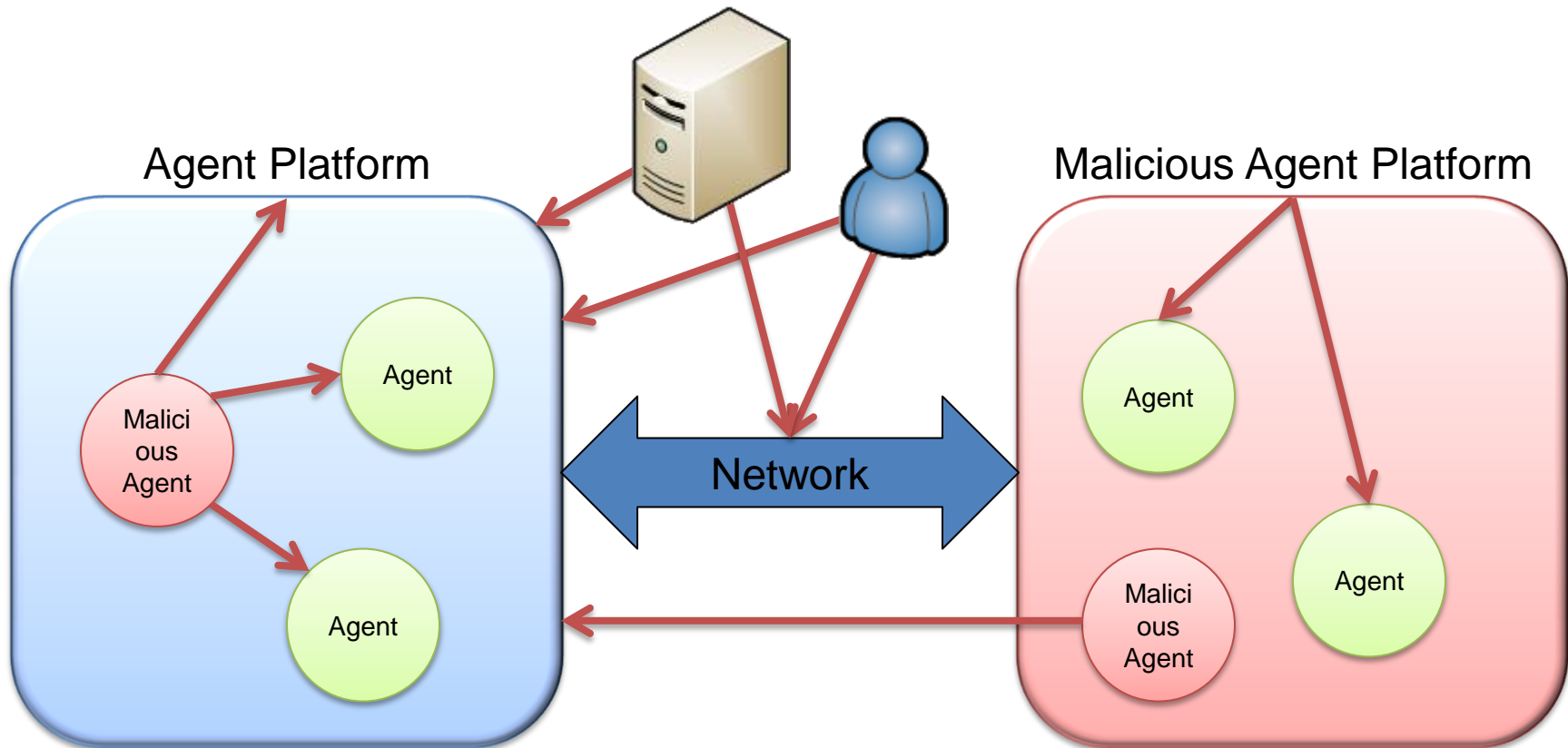
- Network of Agent Execution Environments with specific core components

Agent Security

Agent security must protect against

- Agent vs. Agent
 - Agent attacks another agent in the same platform
- Agent vs. Platform
 - Agent attacks agent platform
- Platform vs. Agent
 - Agent platform attacks agent
- Other vs. Agent
 - Remote agents and other entities attack Agent Platform and Agent Platform communication

Agent Platform Attack Scenarios



Trusted Computing and Mobile Agent Security

Trusted Computing allows

- Identification of platform configuration
- Attestation of platform configuration to remote platform

Trusted Computing establishes

- That a platform is in a trusted configuration
- Which adheres to a specific policy

Policy

- *A policy is a set of rules that constrains the behavior of a device for all conceivable situations [WSB99]*

Trusted Computing Measurement & Attestation

Identification of platform configuration

- Cryptographically secure measurement of the platform

Attestation of platform configuration

- Cryptographically secure report state to remote platform

Based on

- Trusted Platform Module (TPM) for PCs
- Mobile Trusted Module (MTM) for mobile devices

TPM and MTM both have the required capabilities

Trusted Platform Module

Tamper resilient security IC similar to a Smart Card

Provides cryptographic functions

- SHA1 hash
- RSA public key cryptography
- Random number generator

Shielded location protects

- Private keys
- Platform Configuration Registers

Chain of Trust

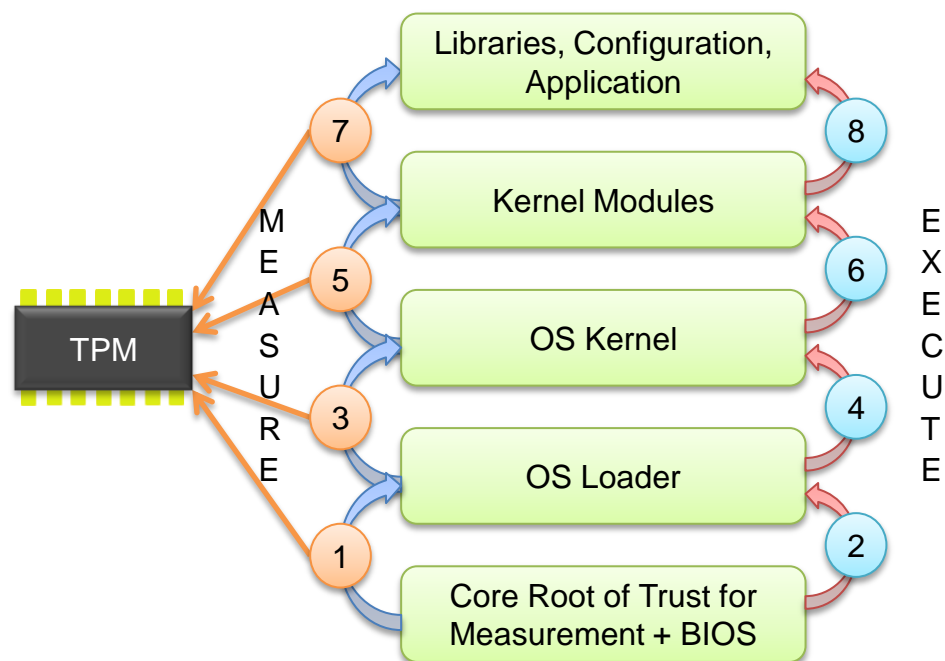
Measurement

- SHA-1 hash of application before execution
- Stored in Platform Configuration Register by hashing old value with new measurement

Chain of Trust

- Core Root of Trust measures BIOS, BIOS boot-loader, boot-loader kernel, ...

Log maintains list of measured components



Remote Attestation

Remote Attestation

- Report the platform configuration to a verifier
- Verifier decides if platform configuration is trusted

TPM Quote:

- TPM signed platform configuration report
 - PCRs are stored in an actual TPM
- Report signed with Attestation Identity Key
 - Alias for unique Endorsement Key of TPM

Mobile Agents in Disaster Response I

Agent Systems in Disaster Response

- Coordination and Support
 - Routing of vehicles, resource allocation
- Information gathering

Disaster strikes and response teams are dispatched

- Equipped with In-Field Devices with TPM
- In-Field Device provides Agent Execution Environment

Command & Control center

- Operates trusted core network
- Might not be available

Mobile Agents in Disaster Response II

Secure, seamless connection of Agent Execution
Environments required

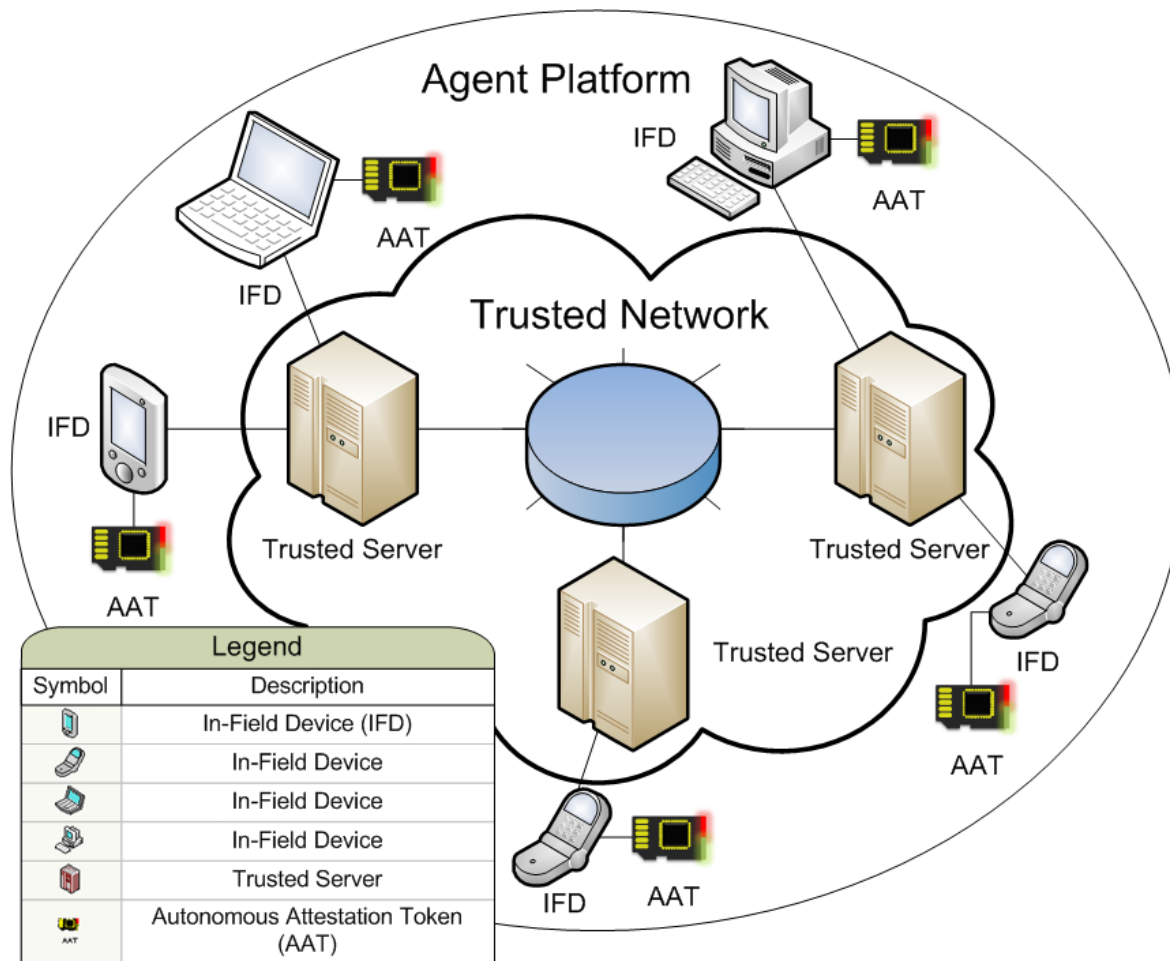
Security important

- Authorization
- Authentication
- **Attestation**
 - Protects against maliciously tampered In-Field Devices

Remote attestation service availability

- Not guaranteed in disaster scenarios

Mobile Agents in Disaster Response Scenario



Autonomous Attestation Token

Autonomous Attestation Token

- Hardware security token
- Many applications for Hardware Security Token
- Basic use case: protects access to the Agent Platform communication key

Agent Platform Key protection

- Local Attestation
- In-Field Device must attest itself to the Autonomous Attestation Token and provide authorization

Local Attestation Properties

True trust decision process

- Works for several devices with several configurations

Eliminates need for remote service

- **Even works if remote service is unavailable**

Deployment of the Autonomous Attestation Token

- Revocation

Maintenance

- Update of In-Field Device implies update of Autonomous Attestation Token

Attestation Based Key Release Protocol

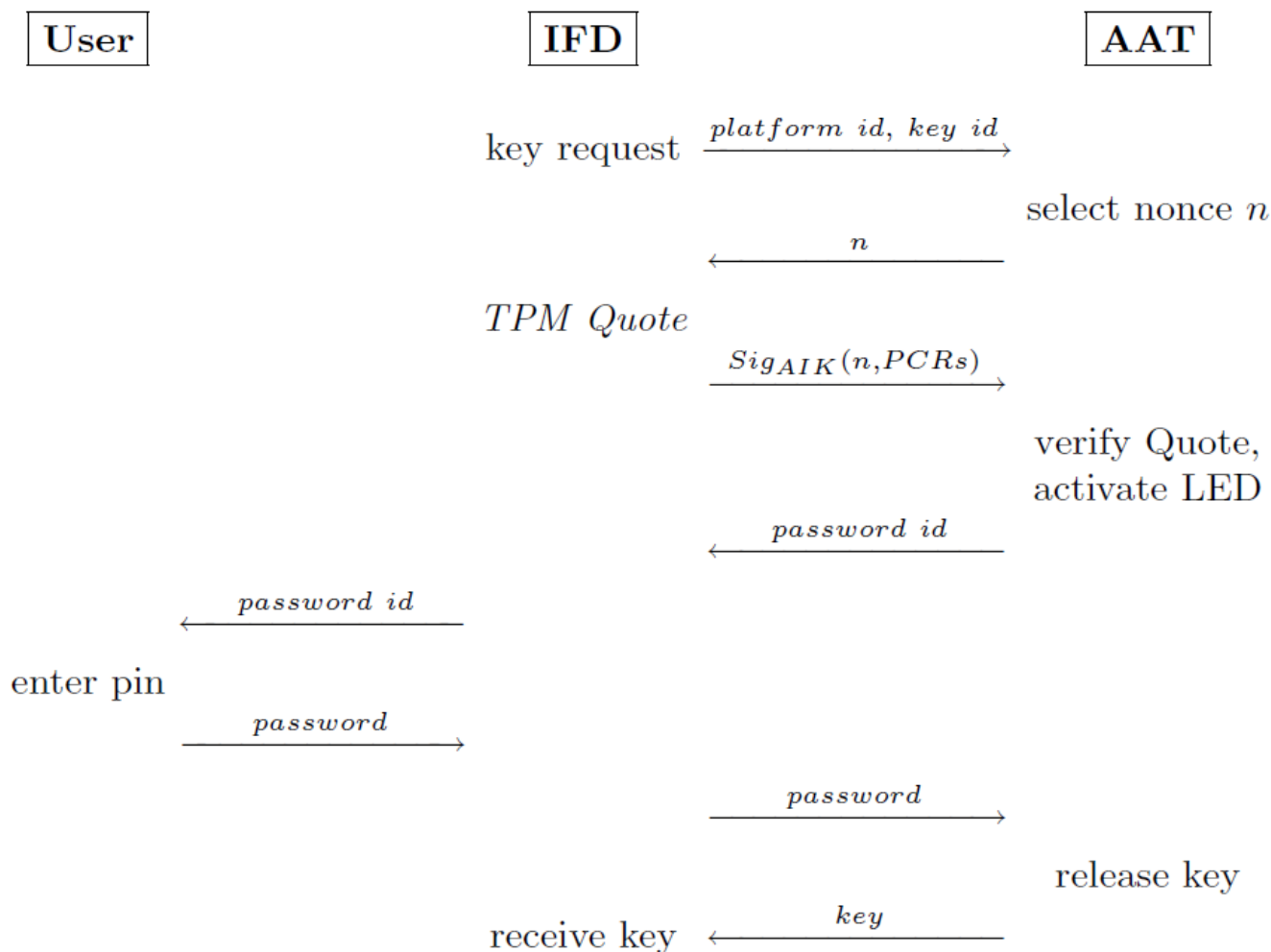
Protect key(s) against

- Unauthorized, malicious entities
- Maliciously modified platforms

Combines

- **Attestation**
 - Without online remote verifier and PKI
- **User interaction**
- **Token specific return channel (LEDs)**

Attestation Based Key Release Protocol



Attestation Based Key Release Protocol I

User wants to connect to Agent Platform

- Requests key from Autonomous Attestation Token

In-Field Device sends key request to attestation token

- Platform ID
 - User might have several platforms
- Key ID
 - AAT is capable of storing several different keys

Autonomous Attestation Token generates nonce

- Nonce guarantees the freshness of the host TPM Quote

Attestation Based Key Release Protocol II

In-Field Device generates TPM Quote

- Sends TPM Quote to Autonomous Attestation Token

Autonomous Attestation Token

- Verifies the quote
 - Signature
 - Nonce
 - Platform Configuration
- If valid
 - Lights green LED
 - Else red LED
 - Requests password

Attestation Based Key Release Protocol III

In-Field Device

- Forwards password request to user

User

- Checks LED and enters short (4 digit) password

Autonomous Attestation Token

- Checks password and if valid releases key

Attestation establishes trust

- User can trust In-Field Device and enter password
- Agent Platform can trust Agent Execution Environment on In-Field Device

AAT Hardware Architecture Requirements I

Hardware optimization goals

- Area (Price)
- Speed
- Energy
- Security (tamper/SCA resilience)

Attestation token protects network access key

- Required once per power cycle

Within certain bounds, execution speed and energy consumption not an issue

Optimize area and security

AAT Hardware Architecture I

Signature verification

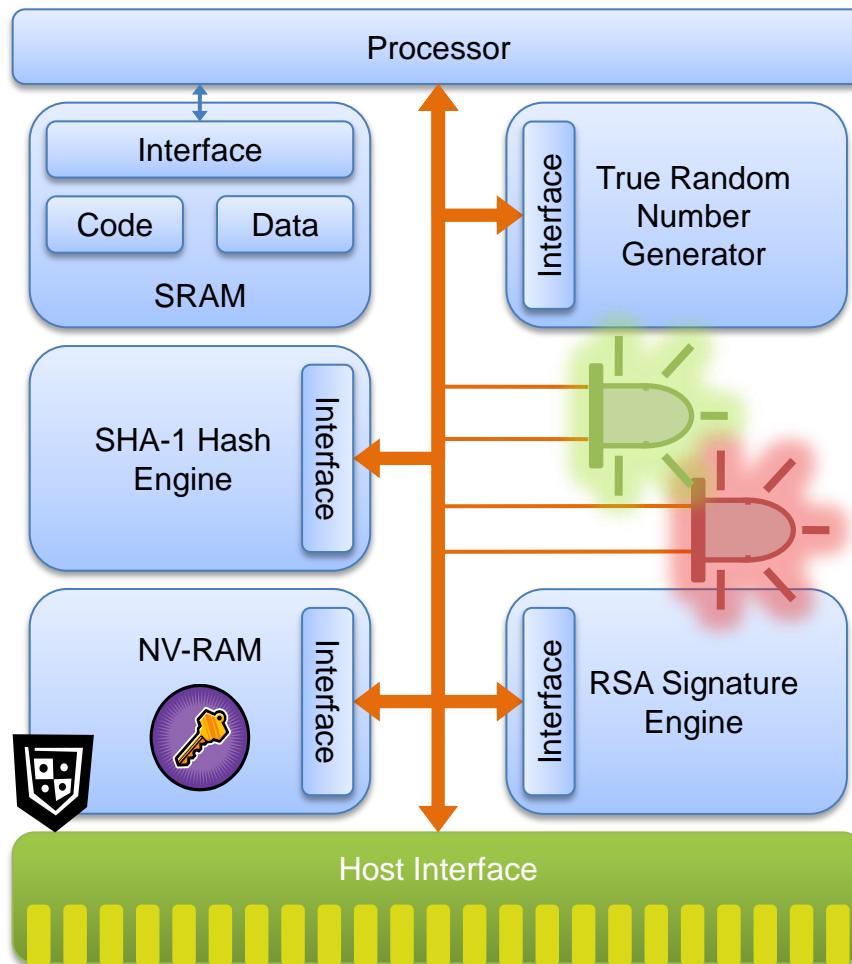
- SHA-1 hash engine
- RSA Signature engine

Shielded key storage

- NV-RAM

Nonce generation

- True Random Number Generator



AAT Hardware Architecture II

Attestation and control

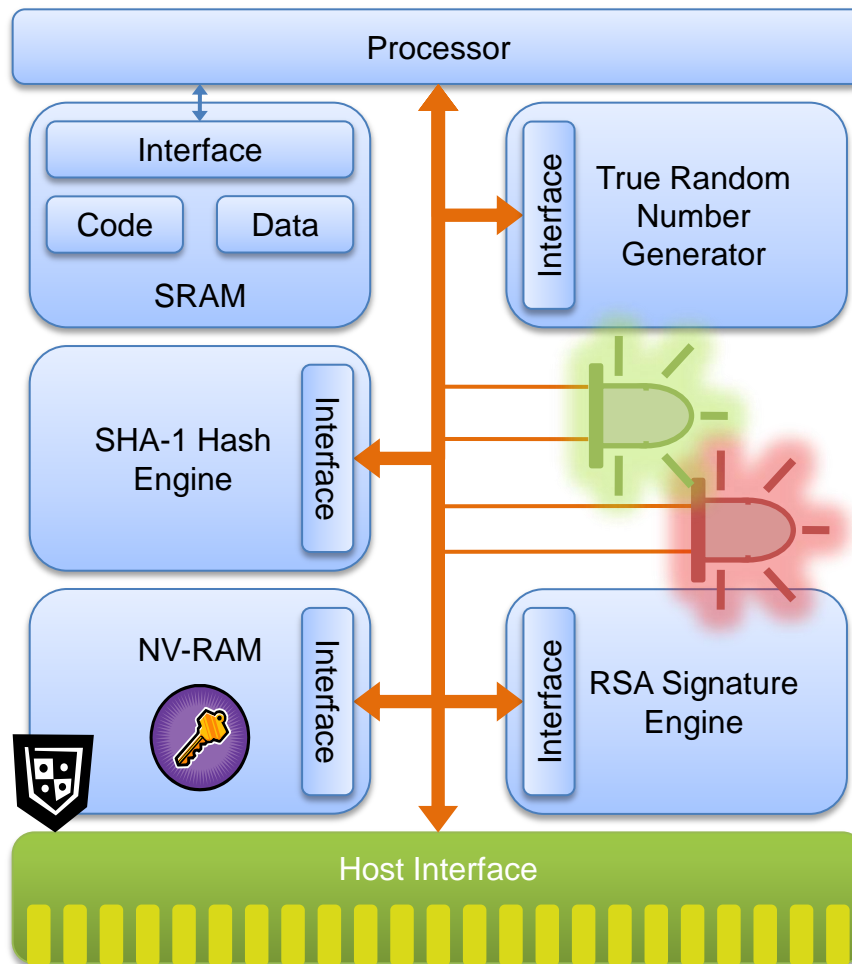
- Processor
- SRAM

Interface

- microSD
- Smart Card
- USB

Trusted path

- Red/Green LEDs



Conclusion

Autonomous Attestation Token

- Hardware security token
 - Simple hardware architecture
- Performs Local Attestation to
 - Establish trust in Agent Execution Environment
 - Limit access to Agent Platform to authenticated and authorized users with an attested platform configuration
- Does not require
 - Online remote verifier and PKI
- Mitigates security risks of Mobile Agent Platforms
- Enables use of Mobile Agents in Disaster Response

Thank you for your attention!



Seamless Communication for Crisis Management (SECRICOM) Open Trusted Computing (Open TC)

This work has been supported by the SECRICOM
and the OPEN-TC projects.

The SECRICOM project is co-financed by the EC
contract no: FP7-SEC-218123

The Open TC project is co-financed by the EC contract
no: FP6-ICT-027635

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

- [RS98] Rothermel, K., Schwehm, M.: Mobile agents. In: A. Kent and J. G. Williams (Eds.): Encyclopedia for Computer Science and Technology, New York: M. Dekker Inc., 1998.
- [WSB99] U. Wilhelm, S. Staamann, and Levente Buttyan. Introducing trusted third parties to the mobile agent paradigm. In Secure Internet Programming: Security Issues for Mobile and Distributed Objects, Lecture Notes in Computer Science (LNCS), pages 471-491, 1999. J. Vitek and C. Jensen, editors, Springer-Verlag (LNCS 1603).